**Affidavit in Support of Application for Search Warrant**

I, Lise B. George, depose and state as follows:

## INTRODUCTION AND AGENT BACKGROUND

1. I have been a Federal Bureau of Investigation ("FBI") Special Agent since 2009. I am currently assigned to violent crime matters within the Providence Resident Agency. I investigate bank robbery, exploitation of children, as well as the trafficking of individuals within and from outside the United States. I have received extensive training in federal criminal and constitutional law and evidence collection. I am a graduate of Georgetown University where I received my master's degree from the School of Foreign Service for Latin American Studies. From 2009 to 2011, I was assigned to a white-collar crime squad where I investigated financial institution fraud, mortgage fraud, and securities fraud among other criminal violations. From 2011 to 2017, I was assigned to the Organized Crime Drug Enforcement Strike Force. From 2017 to 2021, I was assigned to the Boston Field Office where I investigated human trafficking and child exploitation matters. Prior to my appointment as a Special Agent, I was employed for three years as an Intelligence Analyst with the FBI, during which time I conducted analysis, researched, and wrote reports in support of FBI white collar and cybercrime investigations. I have participated in investigations of human trafficking, bank fraud, narcotics trafficking and money laundering, and among other things, have conducted and participated in physical surveillance, debriefings of informants, and the execution of search warrants. I have also been an affiant of Title III wire intercepts.

2. I make this affidavit in support of a search warrant for an iPhone cellular phone that was in the possession of ANTHONY MIELE during a recent vehicle pursuit with the Massachusetts State Police ("MSP"), which ended in ANTHONY MIELE committing suicide. The phone was found with a blue protective case beside ANTHONY MIELE, on the ground of the driver's side of the vehicle. This was the only phone found in the vehicle. The MSP negotiator established communications with MIELE on this phone. The phone is currently located in the Providence, Rhode Island office of the FBI.

3. This affidavit contains specific and articulable facts showing that there are reasonable ground to believe that the contents of the cellular phone are relevant and material to an ongoing criminal investigation into violations of Title 18, United States Code, Sections 2113(a) and (d) makes it a crime for anyone by force and violence, or by intimidation, to take, or attempt to take, from the person or presence of another, any property or money or any other thing of value belonging to, or in the care, custody, control, management, or possession of any federally insured bank and in committing such offense to assault or put in jeopardy the life of any person by the use of a dangerous weapon. I am further aware that Title 18, United States Code, Section 924(c)(1)(A)(ii) makes it a crime to use or carry a firearm during and in relation to a crime of violence. The facts in this affidavit come from my involvement in a collaborative investigation being handled primarily by the FBI, Lincoln Police Department, MSP, Quincy Police Department, Norton, Police Department, Stoneham Police Department and the Easton Police Department. This affidavit is intended to show there are specific and articulable facts for the requested warrant and does not set forth all of my knowledge about this matter.

## SUMMARY OF FACTS

### Citizens Bank- RobberyAttempt, March 15, 2022

4. On March 15, 2022, at approximately 1:38PM there was an attempted robbery at the Citizens Bank, located at 371 Hancock Street, Quincy, Massachusetts. A Quincy Police Department ("QPD") report stated that a white male wearing a dark-colored winter hat, sunglasses, a KN-95 face mask, and a black hoodie approach a victim teller. The suspect held up what appeared to be a state-mailed tax document that had been folded. On a blank surface of the paper, a note was written. The only words that the victim teller noticed was "No Alarms." The victim teller did not give any money to the suspect, and the suspect left still holding the note.

5. After this attempted robbery, QPD conducted a canvass of city cameras and license plate readers. Quincy Detectives identified a vehicle of interest, which was captured by video surveillance in the vicinity of the bank prior to- and post-robbery attempt. The vehicle of interest was identified as a gray Lexus ES, bearing Massachusetts registration 3PPF44 (herein "the Lexus"). The Lexus is registered to THOMAS MIELE, date of birth July 23, 1976 of Northampton, Massachusetts. After reviewing the video footage, the Lexus was captured on camera in the vicinity of Moscow Street and Hancock Street at approximately 1:32PM. At approximately 1:40:39, the Lexus was captured on camera in the vicinity of Billings Road and Hancock Street. At approximately 1:40:55, the Lexus was captured on camera in the vicinity of Hancock Street and Hayward Street. From here, the Lexus is captured leaving Quincy and heading north toward Interstate 93.

### Salem Five Bank Robbery, March 15, 2022

6. On March 15, 2022, the Salem Five Bank, located at 88 Main Street, Stoneham, Massachusetts was robbed. At the time of the robbery, this branch of Salem Five was insured by the FDIC. A Stoneham Police Department ("SPD") report stated in part that at approximately 2:49PM, a white male entered the bank wearing a black, stocking hat, sunglasses, a surgical mask (over his nose and mouth), black gloves, and a tan jacket and tan pants. The male gave a note to the victim teller stating that, "This is a Robbery-No Alarms, No GPS, No Dye Packs. No bait. All the money From top and Bottom Drawer. Do not escalate this situation. Its (sic) all insured and Its (sic) not worth getting hurt over". The loss from the robbery was $564; at the time of the robbery Salem Five was FDIC insured. After the robbery and learning of an attempt at the Citizens Bank that yielded a suspect vehicle, officers canvassed neighboring businesses for video surveillance footage. Officers reviewed video surveillance at the Town Convenient Store located at the corner of Main Street and North Street, approximately 700 feet from the Salem Five Bank. The video surveillance showed the Lexus bearing Massachusetts registration 3PPF44 drive through the parking lot of the store at approximately 2:33PM. In the surveillance video, two people are clearly observed in the Lexus.
7. Subsequently, an analysis conducted at the FBI Laboratory revealed a fingerprint that was lifted from the note used. The fingerprint matched ANTHONY MIELE date of birth 11/1/1972 of Quincy, Massachusetts.
8. After the Citizens Bank attempted robbery and Salem Five Bank robbery, agents and officers conducted surveillance of 514 Washington Street, Quincy, Massachusetts. During the course of the surveillance, both ANTHONY MIELE and THOMAS MIELE were observed together, coming and going from this residence in the Lexus. Surveillance

officers observed Thomas getting into the driver's seat and ANTHONY MIELE getting into the passenger's seat of the Lexus.

9. Given the similarities between the Salem Five bank robbery and the Citizens Bank attempt on March 15, 2022, the presence of the same vehicle at both locations, and that ANTHONY MIELE's fingerprint was lifted from the demand note, I believe that both ANTHONY MIELE and THOMAS MIELE committed these robberies. I believe that the brothers work in concert to commit crimes; specifically that THOMAS MIELE is involved as the getaway driver and ANTHONY MIELE goes inside the bank to commit the robbery.

**Santander Bank June 10, 2022**

10. On June 10, 2022, one man robbed the Santander Bank, located at 622 Washington Highway, #A, Lincoln, Rhode Island. This branch of Santander was insured by the Federal Deposit Insurance Corporation on the day of the robbery.

11. A Lincoln Police Department ("LPD") report includes, in part, the following information: LPD responded to the Santander for a report of a bank robbery. Upon arrival, police met with bank employees, who described the suspect as a man dressed in all black with a black neck gaiter, black cargo pants, a bulletproof vest, a duty belt with OC spray, wearing yellow-lensed sunglasses, and carrying a pair of handcuffs. The suspect was further described as a short male with a tattoo on his hand. The suspect pointed a pistol at the bank employees, dropped a black bag in front of them, and yelled "fill it up!". Another victim teller stated that the suspect was very clam and appeared to know how bank protocol worked. This victim teller stated that the suspect also had an earpiece in his left ear.

**Harbor One Bank, June 16, 2022**

12. On June 16, 2022, one male robbed the Harbor One Bank, located at 472 Foundry Street, North Easton, Massachusetts. At the time of this robbery, this branch of Harbor One was federally insured by the Federal Deposit Insurance Corporation.

13. An Easton Police Department ("EPD") report includes, in part, the following information. On June 16, 2022 at approximately 2:16PM, police were dispatched to HarborOne Bank for a report of a bank robbery. EPD received information that the suspect was dressed in all black, wearing tactical gear similar to a SWAT officer. EPD also received information that the suspect was in possession of a black handgun. EPD collected surveillance footage from a neighboring business captured a BMW grey in color that pulled into the condos at 478 Foundry Street at approximately 2:10PM and then pulled out of the condos at 2:19PM. This timeframe matched the time of the robbery.

14. A victim teller stated that at 2:15PM there were no customers in the bank when an individual dressed in all black clothing walk into the bank. The teller stated that she initially thought the individual was a police officer as she observed him wearing a black knit hat, black tactical style pants, and black boots. The teller also stated that the suspect wore a ballistic type of vest, gloves, and wore a mask that almost covered his entire face. The suspect handed the victim tellers a black drawstring-type bag and told the employees to put all the money in the bag. The employee recalled that the suspect had a firearm in his possession that he waved around and pointed at employees, threatening them. The teller stated that the robber threatened to jump over the desk and force the employees into the safe. The suspect demanded that the tellers open all the drawers, give him the money from the recycler but did not refer to it as the recycler; rather the suspect pointed to it.

The suspect stated, "I'm telling you you're pissing me off…if the police come this is going to turn into a hostage situation and there won't be any hostages." After the teller emptied the "recycler" the suspect fled the bank. The teller believed that the suspect was Caucasian.

15. The affiant reviewed surveillance photos and surveillance video of both robberies. The surveillance footage shows the robber wearing all black, with black gloves, and it shows that he had his finger on the trigger.

16. Given the similarities of the attempt at the Bluestone Bank and the successful robberies of the Santander Bank and HarborOne Bank, and that ANTHONY MIELE was found with the clothing believed to be used in these robberies, I believe that ANTHONY MIELE stole the BMW, possibly with the help of THOMAS MIELE. I believe that both ANTHONY MIELE and THOMAS MIELE committed these robberies. I believe that based on recent collaboration in Massachusetts to rob the Salem Five Bank and the attempt at the Citizens Bank, both ANTHONY and THOMAS MIELE continued to rob banks.

**Deleted Before Sworn.**

## Identification of the Suspect Vehicle

17. On July 18, 2022 video surveillance footage showed a suspicious person, who attempted to enter the Bluestone Bank, located at 225 West Main Street, Norton, Massachusetts. The video surveillance footage showed a male, wearing black tactical clothing, a bulletproof vest, a ski hat, black gloves, a black baklava, black military-style boots, and a duty belt. The surveillance footage also showed a dark-colored BMW leaving the bank at the time that the suspicious person attempted to enter the bank. The footage showed that the BMW had a Connecticut license plate. When case personnel enhanced the footage, a

clear picture of Connecticut registration AC19353, which was stolen from Killingly, Connecticut, was observed. Further, case personnel identified a suspect vehicle that was observed during the robbery at the HarborOne Bank as a 2018 BMW 430Xi, with after-market alterations.

18. Using FBI and Massachusetts Registry of Motor Vehicle databases, MSP identified a list of registered owners of this unique vehicle. On April 27, 2022, a registered owner from Abington, Massachusetts reported his 2018 BMW 430Xi stolen from a convenience store. It was recovered in Quincy, Massachusetts the next day, but without the vehicle's key fob. On May 30, 2022, the same vehicle was stolen again, likely using the key fob that was not recovered from the initial robbery.

19. Case personnel had reasonable belief that this vehicle, with the stolen registration was the same vehicle used in both the Easton bank robbery on June 16, 2022 and the attempt of the Bluestone Bank on July 18, 2022. As a matter of public safety and officer safety, law enforcement issued a BOLO for this vehicle and its operator due to the violent nature of the robberies and the likelihood that the operator of the stolen vehicle was armed.

**Vehicle Pursuit- July 19, 2022**

20. Using Flock safety cameras, a vehicle matching the description of a 2018 BMW 430Xi with Connecticut registration was observed around Lawrence, Massachusetts on July 19, 2022 at approximately 6:13PM. Soon thereafter, law enforcement spotted the vehicle and using their emergency lights, pursued the vehicle to initiate a car stop. The operator did not stop and gave chase to multiple MSP and FBI Bank Robbery Task Force units. Eventually, the vehicle ran out of gas and stopped on Interstate 495 (northbound) in Andover, Massachusetts. When law enforcement approached the vehicle, they observed

the operator put a firearm to his head. Law enforcement retreated, established a perimeter to ensure public safety, and initiated negotiations with the operator of the vehicle. During the negotiation, ANTHONY MIELE provided his cellular telephone number to the MSP negotiator. Later, after a lengthy standoff the operator took his life using a firearm he had in the vehicle. The operator was identified on-scene as ANTHONY MIELE.

21. Case personnel secured consent to search the vehicle that ANTHONY MIELE operated from the registered owner who reported the vehicle stolen twice. During the search, case personnel found a telephone among the belongings of ANTHONY MIELE. Other items found during the search of the vehicle were two pistol magazines, a 9mm Hi-Point firearm, one handheld police radio, a bulletproof vest (without the armored plates), receipts from the Encore Boston Harbor casino in the name of "Anthony Miele," among other items.

ANTHONY MIELE

22. Law enforcement in Massachusetts is familiar with ANTHONY MIELE due to his extensive criminal history, including more than 200 entries on his criminal history. Of those entries, burglary, grand theft, breaking and entering, armed assault, home invasion, assault and battery, assault to murder, and intimidation were reported within the last eight years. Most of these charges are in Massachusetts but he had criminal charges in Florida, as well.

THOMAS MIELE

23. Law enforcement in Massachusetts is familiar with THOMAS MIELE due to multiple entries on his criminal history, to include possession of a firearm, possession of a firearm in commission of a felony, possession of heroin, possession of a sawed-off shotgun,

trafficking cocaine and heroin, among other entries. These charges are out of Massachusetts courts.

24. Based on my training and experience, I believe that many bank robbers use a "getaway driver" and work in pairs to evade law enforcement. I believe that based on both the criminal histories, which include many entries for larcenies, breaking and entering, and assaults, they may have been involved in other robberies as well. I believe that given the recent attempt and successful robbery in Stoneham, ANTHONY MIELE may have been working in concert with THOMAS MIELE to rob the Santander Bank in Lincoln, Rhode Island and the HarborOne Bank in Easton, Massachusetts. I believe that evidence of this collaboration, specifically text conversations about planning, conduct prior and after the bank robbery, and evidence of what was done with the stolen money may be found on ANTHONY MIELE's phone. I believe that text conversations on messaging applications, call log details, photos, videos, among other evidence, exist that show ANTHONY and THOMAS MIELE conspired to rob the banks mentioned in this affidavit. I also believe that evidence exists that show THOMAS MIELE's involvement in other unsolved bank robberies. I believe that this evidence may detail THOMAS MIELE's role as the getaway driver and provide case personnel a better idea of their role in previously unsolved criminal behavior in Rhode Island and Massachusetts.

**TRAINING AND EXPERIENCE ON DIGITAL DEVICES**

25. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

26. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

27. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

28. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

    a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

    b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

29. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

## Conclusion

30. I believe that there are fruits of the crime on the cell phone to include information about previously unsolved bank robberies and possible other criminal activity. Based on my training and experience, I also believe that ANTHONY MIELE might have acted in concert with THOMAS MIELE (and/or other criminal actors) and that evidence of that collaboration may be on his cellular phone.

Respectfully submitted,

Lise B. George, Special Agent
Federal Bureau of Investigation

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone
*(specify reliable electronic means)*

**Sworn telephonically and signed electronically**

August 9, 2022
*Date*

*Judge's signature*

Providence, Rhode Island
*City and State*

**Patricia A. Sullivan, USMJ**
*Patricia A. Sullivan, U.S. Magistrate Judge*

**ATTACHMENT A**

This warrant applies to the cellular telephone found on the floor of the driver's side of the vehicle that was driven by ANTHONY MIELE on July 19, 2022. The cellular telephone is described as a black iPhone with a blue case. The phone is located at the Providence Resident Agency of the FBI, 10 Weybosset Street, Providence, Rhode Island.

# ATTACHMENT B

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as a means of committing a criminal offense, namely violations of 18 U.S.C. § 2113(a) and (d); Title 18, U.S.C. § 924(c)(1)(A)(ii) makes it a crime to use or carry a firearm during and in relation to a crime of violence (the "Specified Federal Offenses"):

1. Records, information, and items relating to any communications by, between and among, and/or relating to the SUBJECT PERSONS (ANTHONY MIELE and THOMAS MIELE) and known and unknown conspirators and witting or unwitting accomplices, relating to the Specified Federal Offenses, via any social media, online account, and communications platforms, including but not limited to Snapchat, Instagram, Facebook, Facebook Messenger, Pinterest, FaceTime, Skype, email, telephone, and any SMS and MMS messaging platforms, including WhatsApp and Telegram.

2. Records, information, and items relating to acquisition and use of guns and/or firearms.

3. Records, information, and items relating to acquisition and use of police/military-type uniforms, equipment, and/or clothing.

4. Photographs, videos, images, and other media of the fruits of the criminal behavior committed by SUJECT PERSONS.

5. Records, information, and items relating to the opening of, use, and access of casino accounts in the names of the SUBJECT PERSONS and known and unknown conspirators and witting or unwitting accomplices.

6. Records, information, and items relating to the deposit of cash, and any and all bank statements, transaction records, and ATM receipts for such accounts.

7. Records, information, and items relating to the recruitment or solicitation of persons to assist in the aforementioned bank robberies and other robberies, break-ins, grand-thefts, and other criminal behavior by the SUBJECT PERSONS, and offers to pay or payments for recruitment.

8. Records, information, and items relating to banking and financial accounts and records of or relating to the SUBJECT PERSON, and known and unknown co-conspirators and witting or unwitting accomplices, used in furtherance of the Specified Federal Offenses, and known and unknown conspirators, and their nominees, assignees, including bank statements,

deposit tickets, deposit items, checks, money orders, cashier's checks, official checks, bank drafts, wire transfer instructions and receipts, checkbooks, check registers, passbooks, withdrawal slips, credit memos, debit memos, signature cards, account applications, automatic teller machine receipts, safe deposit box applications, safe deposit box keys, pre-paid debit and credit cards, debit and credit card statements, charge slips, receipts, financial statements, balance sheets, income statements, cash flow statements, ledgers, journals, accounts receivable, accounts payable, leases, brokerage statements, and any other items evidencing the obtaining, disposition, secreting, transfer, or concealment of assets.

9. Records, information, and items relating to the access and use of money service businesses, such as Western Union and/or Moneygram; online bank transfer services, such as Zelle, Venmo, Cash App, or Paypal; and cryptocurrency accounts and cryptocurrency exchanges, such as BitCoin.

10. Records, information, and items relating to Global Positioning System ("GPS") coordinates and use of GPS mapping systems that identify persons, places, and information that constitute evidence of the commission the Specified Federal Offenses.

11. Records, information, and items records reflecting the identity of, contact information for, communications with, or times, dates or locations of meetings with co-conspirators and witting or unwitting accomplices, involved in the Specified Federal Offenses, including calendars, address books, telephone or other contact lists, correspondence, receipts, and wire transfer or fund disposition records, and communications relating to the same.

12. Records, documents, and deeds reflecting the purchase or lease of real estate, vehicles, precious metals, jewelry, or other items obtained with proceeds from criminal activity specified in this affidavit.

13. For any computer, cellular or digital device, cellular telephone, and/or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information whose seizure is authorized by this warrant, including any cell phones (hereinafter, "DIGITAL DEVICE")[1]:

[1] The term "DIGITAL DEVICE" includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile/cellular phones, tablets, server computers, and network hardware. The term "storage medium" includes any physical object upon which computer data can be

a. evidence of who used, owned, or controlled the DIGITAL DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved user names and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
b. evidence of software that would allow others to control the DIGITAL DEVICE, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
c. evidence of the lack of such malicious software;
d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crimes under investigation and to the computer user;
e. evidence indicating the computer user's knowledge and/or intent as it relates to the crimes under investigation;
f. evidence of the attachment to the DIGITAL DEVICE of other storage devices or similar containers for electronic evidence;
g. evidence of programs (and associated data) that are designed to eliminate data from the DIGITAL DEVICE;
h. evidence of the times the DIGITAL DEVICE was used;
i. passwords, encryption keys, and other access devices that may be necessary to access the DIGITAL DEVICE;
j. documentation and manuals that may be necessary to access the DIGITAL DEVICE or to conduct a forensic examination of the DIGITAL DEVICE;
k. records of or information about Internet Protocol addresses used by the DIGITAL DEVICE; and
l. records of or information about the DIGITAL DEVICE's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

14. With respect to any and all electronically stored information in cellular telephones and cellular devices, in addition to the information described herein, agents may also access, record and seize the following information to the extent that it identifies persons, places, and information that constitute evidence of the commission the Specified Federal Offenses:
a. Telephone numbers of incoming/outgoing calls stored in the call registry;
b. Digital, cellular and/or telephone numbers and/or direct connect numbers, names and identities stored in the directories;

---

recorded. Examples include hard disks, external drives, RAM, flash memory, CD-ROMS, memory sticks, USB drives, and other magnetic or optical media.

c. Any incoming/outgoing text messages relating to the above criminal violations;
d. Telephone subscriber information;
e. The telephone numbers stored in the cellular telephone and/or PDA;
f. Records relating to the use, possession, and control of any cellular telephones and cellular devices seized;
g. Any other electronic information stored in the memory and/or accessed by the active electronic features of the digital or cellular telephone including photographs, videos, e-mail, and voice mail relating to the above Specified Federal Offenses.

15. Contextual information necessary to understand the evidence described in this attachment.

II. AUTHORIZED SEARCH PROCEDURE

1. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location.

2. In order to search for the items described above that may be maintained in electronic media, the search team are authorized to search, copy, image and seize the following items for off-site review:
   a. Any computer or storage medium capable of being used to commit further or store evidence of the Specified Federal Offenses; and
   b. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer or storage medium;

3. Pursuant to Rule 41(f)(1)(B), the government will retain a copy of the electronically stored information that was seized or copied for the purpose of the evidentiary authentication and any potential discovery obligations in any related prosecution.